UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,667	06/28/2001	Luke E. Girard	219.40075X00	2051

23838 7590 01/24/2007
KENYON & KENYON LLP
1500 K STREET N.W.
SUITE 700
WASHINGTON, DC 20005

EXAMINER	
POLTORAK, PIOTR	
ART UNIT	**PAPER NUMBER**
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 09/892,667	**Applicant(s)** GIRARD, LUKE E.	
	Examiner Peter Poltorak	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's Amendment received on submission filed on 12/04/06 has been entered.
2. The independent claims 1, 15 and 24 and dependent claims 3, 7, 16 and 26 have been amended.
3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

4. Claims 1-26 have been examined.

Response to Amendment

5. Applicant's remarks have been carefully considered.
6. In light of applicant's amendments the previously stated objections and USC § 112 rejections have been withdrawn.
7. Applicant arguments are directed towards a newly introduced limitation. Specifically applicant argues that Cromer does not disclose system login authentication or system login security policies and determining whether a mobile system may have been stolen or used inappropriately based on the system login security policies.
   In order to underline the alleged Cromer's deficiencies, applicant suggests that "if the system of Cromer is located outside of an authorized area, it is deemed stolen and immediately disabled. There is no further need for Cromer to make a determination based on the system login security policies, because once the system moves outside of the designated area, it is disabled".

8. The new limitation is addressed in the current Office Action, below. However, the examiner points out that the specification does not disclose how system login security policies would be used to determine whether a mobile system is stolen. Claims 16 and 26 address log-on security policies explicitly reciting failed log-on attempts. However, it is not clear, how log-on attempts would enable one to determine that a device is stolen, in particular since it is uncommon for users to forget/mistype their password. Although the specification provide some implicit examples of security policies, e.g. "location of logon such as an Internet Protocol (I.P.) address, paragraph 38 of the specification detailed description) it is not completely clear that policies derived from these examples would read on applicant's definition of "system login security policies" especially since applicant does not elaborate on relationship of these examples to login policies. Thus, for purposes of the examination the examiner focuses on the phrase "**may have been** stolen **or** used inappropriately". It appears that an unexpected input directed towards logon to a system (e.g. wrong login credentials such as password or user name, a repeated login attempt or attempt during unauthorized time etc.) would meet the claim limitation as long as it could have the same results when attempted by an unauthorized user (e.g. incorrect credentials provided by an unauthorized user). Such an interpretation is disclosed by Hadfield, as discussed in this Office Action, below.

Furthermore, as per argument that Cromer would no further need make a determination based on system login security policies because of disabling the system that is moved outside of the designated, the examiner points applicant to col. 3 lines 39-41, in which Cromer clearly disclose that user authentication and area "validity" are both taken in consideration before a user can work with a device.

9. Claims 1-26 have been examined.

Rejections - 35 USC § 103

10. Claims 1-2 are rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213).*

As per claims 1-2 *Cromer* discloses a mobile system *(Cromer, Fig. 1)* comprising a host chipset, a locator susbsystem connected to the host chipset and arranged to determine a current location of the mobile system and a main storage connected to the host chipset *(Cromer, Fig. 2, col. 4 line 53 - col. 5 line 50).*

Cromer discloses enforcing security policies during user authentication, to access the locator subsystem and determine whether the mobile system may have been stolen or used inappropriately based on the current location of the mobile system and the security policies *(Cromer, col. 3 lines 42-col. 4 lines 16).*

Cromer does not explicitly disclose that the main storage is arranged to store an operating system (OS) and that it contains an OS-Present application. However, computers, including mobile computers, inherently use OS and most of the every commercial laptops contain an OS-Present applications. Thus the use of an OS-Present applications in *Cromer's* mobile device, would have at least been obvious given the fact that OS-Present applications provide extend devices functionalities beyond simply booting up the device. Furthermore, mobile devices such as laptops inherently use main memory to store OS, and the OS-Present application and flash memory to store Pre-OS application that are executed during boot up. In fact, Cromer explicitly discloses a flash memory arranged to store the Pre-OS application, which is executed during boot-up before the operating system (OS) is loaded *(Cromer, col. 5 lines 13-18).*

11. Cromer does not disclose system login security policies that are enforced. *Hadfield* teaches login security policies (number of failed log-on, *"Account Policy", Handfield, pg. 28 and "Account and Password Security", pg. 301-305*).
It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a login security policies such as designated number of failed log-on attempts given the benefit of increase security preventing repeated log-on attempts by someone trying to guess an account password *("Account Policy", Handfield, pg. 28 and "Account and Password Security", pg. 303).*

12. On page 304 Handfield discloses enforcing the login security policy preventing security attacks (Account lockouts, Handfield, pg. 303-304).

Claim Rejections - 35 USC § 103

13. Claims 3-6 are rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* and further in view of *Angelo (U.S. Patent No. 6581162).*

Cromer discloses a mobile system wherein the locater subsystem is a radio frequency based locator subsystem for determining the current location of the mobile system *(Cromer, col. 3 lines 42-44).*

14. *Cromer* does not explicitly disclose that the Pre-OS application and the OS-Present application are supported by a protected storage configured that stores configuration data, the security polices, authentication data and other information obtained from the Pre-OS applications and the OS-Present application.

    Angelo discloses a protected storage configured to store sensitive data such as authentication data *(Angelo, col. 2 line 66- col. 3 line 40).*

    It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement a protected storage configured to store sensitive data such as authentication data as disclosed by *Angelo* to support the Pre-OS and OS-Present applications disclosed by *Cromer*. One of ordinary skill in the art would have been motivated to perform such a modification given the benefit of preventing security breaches *(Angelo, col. 2 lines 39-64).*

15. Although *Angelo* does not explicitly discloses storing in the protected storage other information such as configuration data and the security policies, storing any of this type of data would not affect the functionality of the invention and in fact would have been obvious to one of ordinary skill in the art at the time of applicant's invention given the benefit of protecting confidentiality of the sensitive information.

16. The limitations of claim 4, if not inherent, are at least implicit. In computing, applications communicate with objects (e.g. locations, routines etc.) via interfaces that vary depending on an application layer.

17. Claim 5 is inherent: password authentication involves comparing a user-entered password with an entry previously stored in the authenticating computer.

18. Claim 7 is rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* and *Angelo (U.S. Patent No. 6581162)* and further in view of *Patel (U.S. Patent No. 6438690)*.

    Cromer in view of *Angelo* teach a mobile enforcing system security polices such as system logon security policies for the Pre-OS and/or the OS-Present application, as discussed above. Furthermore, *Hadfield* discloses other examples of system security policies: unauthorized use of monitored services and an unauthorized change attempted on selected platform policies *("Rights policy", and individual properties that each user account will have, Hadfield, pg. 27-28)* and designated time expiration (e.g. Hadfield, Fig. 13.5 on pg. 303).

    Cromer in view of *Angelo* do not explicitly teach time expiration based on a renewable certificate.

    Patel discloses renewable certificates used in authorizing access *(e.g. Patel, col. 2 lines 24-39 and col. 7 lines 45-48)* and discloses time expiration based on a renewable certificate *(Patel, col. 2 lines 13-23)*.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include time expiration based on a renewable certificate as disclosed by *Patel* given the benefit of increased security *(Patel, col. 2 lines 1-10).*

19. Additionally, the examiner points out that the recited security policies are only found in the nonfunctional descriptive material and are not functionally involved in the steps recited. Enforcing security policies would be performed regardless of the type of policies implemented. Thus, this descriptive material will not distinguish the claimed invention from the prior art in terms of patentability, see In re Gulack, 703 F.2d 1381, 1385, 217 USPQ 401, 404 (Fed. Cir. 1983); In re Lowry, 32 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994).

20. Claims 15, 21-22 and 24 are rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* and further in view of *Rainbow Technologies (Rainbow Technologies, "Protecting Laptops with iKey and Intel Protected Access Architecture").*

Cromer in view of *Hadfield* enforcing system login security policies during user authentication and discloses Pre-OS BIOS instructions *(e.g. Cromer, col. 5 lines 13-18)* that inherently implement initializing and testing a system platform but is silent in regard to BIOS instructions being configured in accordance with IPAA enforcing security.

Rainbow Technologies teach a system basic input/output start-up being configured in accordance with IPAA and being executed during boot up and enforcing security policies before the OS is loaded *(Rainbow Technologies, "How Does IPAA Work section, pg. 2)*.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement a system basic input/output start-up being configured in accordance with IPAA and being executed during boot up before the OS is loaded as taught by *Rainbow Technologies.* One of ordinary skill in the art would have been motivated to perform such a modification in order to make a stolen laptop unusable by unauthorized users *(Rainbow Technologies, The Intel Protected Access Architecture section, pg. 2)*.

21. The examiner also points out that an ordinary artisan would appreciate authentication enhancements provided by IPAA technology preventing affections or bypassing by rogue software and data reset *(Rainbow Technologies, "The Intel Protected Access Architecture (IPAA), pg. 2)*.

22. As per claim 21-22 *Cromer* discloses a GPS receiver/transmitter *(Cromer, col. 3 lines 42-43)*.

23. Claims 20 and 25 are rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* and *Rainbow Technologies (Rainbow Technologies, "Protecting Laptops with iKey and Intel Protected Access Architecture")* and further in view of *Cotichini (U.S. Patent No. 6300863)*.

Cromer in view of *Hadfield* and *Rainbow Technologies* disclose BIOS instructions as discussed previously but fail to disclose reporting the location based information indicating the current location of the mobile system to a proper authority, via an Internet or a RF-based wireless network.

Cotichini discloses reporting the location based information indicating the current location of the mobile system to a proper authority, via an Internet or a RF-based wireless network *(Cotichini, Abstract, col. 10 line 56-col. 11 line 31).*

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include reporting the location based information indicating the current location of the mobile system to a proper authority, via an Internet or a RF-based wireless network given the benefit of recovering the mobile system *(col. 28 lines 15-21).*

24. Claim 26 is rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* and *Rainbow Technologies (Rainbow Technologies, "Protecting Laptops with iKey and Intel Protected Access Architecture")* and further in view of *Patel (U.S. Patent No. 6438690).*

25. Claim 26 introduces limitations substantially equivalent to the limitations of claim 7; therefore claim 26 is similarly rejected.

26. Claims 8-9 are rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler,*

"Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213), Angelo (U.S. Patent No. 6581162), and *Patel (U.S. Patent No. 6438690)* and further in view of in view of *Rainbow Technologies (Rainbow Technologies, "Protecting Laptops with iKey and Intel Protected Access Architecture")*.

Cromer, Hadfield, Angelo and Patel teach the mobile device security as discussed above including collecting location based information from the RF-based locator subsystem and making decision that the mobile system may have been stolen or used inappropriately based on a violation of the security policies.

27. *Cromer, Hadfield, Angelo and Patel* do not teach that BIOS is configured in accordance with IPAA. However, this limitation in claim 8 is substantially equivalent to the limitation of claim 25; thus it is similarly rejected.

28. Claim 10 is rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213), Patel (U.S. Patent No. 6438690), Angelo (U.S. Patent No. 6581162)* and *Rainbow Technologies (Rainbow Technologies, "Protecting Laptops with iKey and Intel Protected Access Architecture")* and further in view of *Cotichini (U.S. Patent No. 6300863).*

Claim 10 introduces limitations substantially equivalent to the limitations of claim 25; therefore claim 10 is similarly rejected.

29. Claims 11-13 are rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213), Patel (U.S.*

Patent No. 6438690), *Angelo (U.S. Patent No. 6581162)* and *Patel (U.S. Patent No. 6438690)* and further in view of *Cotichini (U.S. Patent No. 6300863).*

Claim 11 introduces limitations substantially equivalent to the limitations of claim 25; therefore claim 11 is similarly rejected.

30. As per claim 13 GPS systems utilize radio towers but *Cromer, Angelo, Hadfield* and *Patel* do not explicitly disclose that the broadcasted signal is silent. However, *Cromer, Angelo, Hadfield* and *Patel* do not mention anything about an audio (non-silent) signal and RF, and unless purposely modified while received by output devices, signals are silent. Furthermore, Official Notice is taken that it is old and well-known practice sending a silent signal in situation where unauthorized actions are suspected. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to broadcast signal in order not to alert a potential unauthorized person to the fact that the mobile device is traced by authorities.

31. Claims 16-18 are rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* and *Rainbow Technologies (Rainbow Technologies, "Protecting Laptops with iKey and Intel Protected Access Architecture")* and further in view of *Patel (U.S. Patent No. 6438690).*

Claim 16 introduces limitations substantially equivalent to the limitations of claim 7; therefore claim 16 is similarly rejected.

32. Claims 19 are rejected under 35 U.S.C. 103(a) as obvious over Cromer *(U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213), Rainbow Technologies (Rainbow Technologies, "Protecting Laptops with iKey and Intel Protected Access Architecture")* and *Patel (U.S. Patent No. 6438690)*, and further in view of *Cotichini (U.S. Patent No. 6300863).*

    Claim 19 introduces limitations substantially equivalent to the limitations of claim 25; therefore claim 19 is similarly rejected.

33. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over are rejected under 35 U.S.C. 103(a) as obvious over *Cromer (U.S. Patent No. 6166688)* in view of *Hadfield (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213)* in view of *Rainbow Technologies (Rainbow Technologies, "Protecting Laptops with iKey and Intel Protected Access Architecture")* and further in view of *Bajikar (U.S. Pub. 20020194500).*

    Cromer in view *Hadfield* and *Rainbow Technologies* teach the mobile system as discussed above.

    Cromer in view of *Hadfield* and *Rainbow Technologies* do not teach the RF-based locator subsystem corresponding to a Bluetooth TM transceiver that is part of a Bluetooth TM based security system including a central security server and a network of Bluetooth (voice/data) Access Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control, remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network.

Bajikar teaches a Bluetooth based security system utilized to provide ad-hoc security services to secured assets comprising a secured device (SD) equipped with Bluetooth (BT) technology; a plurality of Bluetooth Access Points (BTAPs) located at designated points to establish a BT link with the secured device (SD); and a security server (SS) connected to all BTAPs and arranged to provide access control and security services for the secured device (SD), wherein the security server (SS) obtains attribute information *(Abstract and Fig. 1)*. Furthermore *Bajikar* discloses that the Bluetooth TM based security system serves to control and monitor the status of all secured devices or assets remotely, through the Internet or other networks *[0024]*.

The *Bajikar's* teaching reads on RF-based locator subsystem corresponding to a Bluetooth TM transceiver that is part of a Bluetooth TM based security system including a central security server and a network of Bluetooth (voice/data) Access Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control, remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to utilize an RF-based locator subsystem subsystem corresponding to a Bluetooth TM transceiver that is part of a Bluetooth TM based security system including a central security server and a network of Bluetooth (voice/data) Access

Points (BTAPs) installed in a designated area to provide security services for the mobile system, including asset control, remote monitoring and tracking of the mobile system, through the Internet or the RF-based wireless network as taught by *Bajikar*. One of ordinary skill in the art would have been motivated to perform such a modification in order to provide low-cost and low-power ad-hoc security *[Bajikar 0021]*.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-

3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

1/8/07

KAMBIZ ZAND
PRIMARY EXAMINER